REMARKS

This Amendment responds to the Office Action dated June 30, 2006. It is noted that in this latest Office Action all of the prior rejections were withdrawn in view of the Appeal Brief filed on March 30, 2006. The rejections contained in this latest Office Action are based on a newly-cited reference, US 5,956,404 to Schneier. All of these new rejections are traversed for the reasons noted below.

A) Interview Summary

An interview was conducted between the Examiner and the undersigned representative on September 12, 2006. During the interview, the language of claim 1 was discussed and the undersigned representative agreed to amend the claim language to clarify the relationship between the use of the ephemeral key pair in the encrypting and generating steps.

B) Request for Information under 37 C.F.R. § 1.105

The Examiner requested that applicants "disclose all patents and applications for patents in the United States as well as any other foreign countries they may have filed in." This requests is interpreted to mean all patents and applications that are directly related to this application. As such, the assignee of the present application has filed related applications in Canada and the European Patent Office. Both of these applications have been granted. The Canadian patent is CA 2,312,331 and the EPO patent is EP 1063813. A copy of each of these granted patents is included herewith in an accompanying IDS submission.

C) Rejection Under 35 U.S.C. § 102

Claims 1, 16 and 31 were rejected in the latest Office Action over the Background section of the Schneier reference, specifically at column 1, lines 28-65. This portion of Schneier is set forth below.

The public-private key encryption technique has resolved the above-identified problem. Based on a public-key/private-key key pair, every digital message can be encrypted by any one of the key and decrypted by the other, with the public keys recorded in a public directory, which is publicly accessible, and the private key privately retained. Typically, the sender of the message would go to the public-key directory to look for the receiver's public key. Then the sender would encrypt the message with the receiver's public key, and convey the encrypted message to the receiver. The receiver, upon getting the encrypted message, decrypts the message with her private key. Such a public-private key scheme resolves the problem of maintaining the secrecy of a communication. However, when the receiver gets the message, the receiver cannot be certain that the message is from the sender. The receiver would like to have the equivalence of a signature on the message.

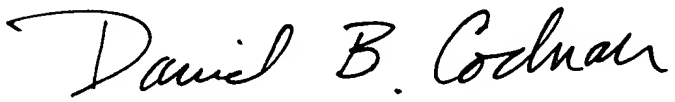
The public-private key encryption technique can also be used to generate a digital signature to authenticate the sender. Typically, the sender would hash the message with a one-way hashing function that is publicly known and is an agreed-upon standard, such as published in the newspaper. Hashing a message is a computation applied to a message that collapses the message and transforms it to a unique value—no two messages have the same value. After hashing, the sender would digitally sign the message by encrypting the hashed message with her private key. Both the digital signature and the message will be encrypted by the receiver's public key, and are then sent to the receiver. The receiver, upon getting the information, decrypts it, and extracts the digital signature from it. Then the receiver gets the sender's public key from the public directory to decrypt the digital signature to get back the same message. This operation ensures the identity of the sender because she is the only person who can encrypt the message with her private key. One cryptosystem that allows digital signatures with message-recovery is RSA. There are also ElGamal variants, which allow signing with message recovery.

As can be seen from reading this text, the Background section of Schneier is merely describing the prior art encryption and digital signature steps. Lines 28-45 of this text describes the well-known public-private key encryption process discussed in relation to Figure 1 of the present application, and lines 45-65 describes the well-known digital signature process discussed in relation to Figure 2 of the present application.

What is missing from this relied-upon text, however, is any mention at all of producing an "ephemeral" key pair. The key generating steps discussed in Schneier are static key pairs, they are not "ephemeral," or "temporary." In addition, there is no disclosure in this portion of Schneier of producing such an "ephemeral" key pair that is used to encrypt a plaintext message

into a ciphertext message, and then subsequently generating a digital signature for the ciphertext message using the same ephemeral key pair that was used to encrypt the plaintext message. Therefore, amended claims 1, 16 and 31 are clearly distinguishable from this portion of the cited reference and thus all of the claims are in condition for allowance.

Respectfully submitted:



JONES DAY
David B. Cochran
Reg. No. 39,142
901 Lakeside Ave.
Cleveland Ohio, 44114
216-586-7029
dcochran@jonesday.com